



PATENT  
Attorney Docket No. 81942.0004  
Customer No. 26021

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Kiyoshi OGISHI, et al.

Serial No: 09/708,263

Filed: November 7, 2000

For: Key Sharing Method, Secret Key  
Generating Method, Common Key  
Generating Method and  
Cryptographic Communication  
Method in ID-NIKS Cryptosystem

Art Unit: 2134

Examiner: Jung, David Yiuk

Confirmation No: 9975

**TRANSMITTAL OF  
INFORMATION DISCLOSURE STATEMENT**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

I hereby certify that this correspondence  
is being deposited with the United States  
Postal Service with sufficient postage as  
first class mail in an envelope addressed  
to:

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450, on  
February 8, 2006

Date of Deposit

Juanita Soberanis

Name

*Juanita Soberanis* 2/08/2006

Signature

Date

Dear Sirs:

1. ☒ The information disclosure statement submitted herewith is being filed within three months of the filing date of the application other than a continued prosecution application, or within three months of the date of entry into the national stage of an international application, or before the mailing date of a first Office Action on the merits, or before the mailing of a first Office action after the filing of a request for continued examination under §1.114, whichever event occurs last. 37 C.F.R. §1.97(b).
2. ☐ The information disclosure statement transmitted herewith is being filed *after* the period specified in §1.97(b), but *before* the mailing date of a final action under §1.113, or a notice of allowance under §1.311, or an action that otherwise closes prosecution in the application, whichever occurs first. A statement specified in §1.97(e) or a fee set forth in §1.17(p) is included. 37 C.F.R. §1.97(c).

**§1.97(e) STATEMENT**

I, the person signing below, state:

- ☐ that each item of information contained in the information disclosure statement was first cited in the attached communication from a foreign patent office in a counterpart foreign application and that the communication is dated not more than three months prior to the filing of the statement. 37 C.F.R. §1.97(e)(1).

OR

- ☐ that no item of information contained in the information disclosure

statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in §1.56(c) more than three months prior to the filing of the statement. 37 C.F.R. §1.97(e)(2).

**OR FEE**

- ☐ Attached is a fee set forth in 37 C.F.R. §1.17(p) for submission of an information disclosure statement under §1.97(c). (\$180.00). [OR:] Please charge the fee set forth in 37 C.F.R. §1.17(p) for submission of an information disclosure statement under §1.97(c) (\$180.00) to Deposit Account No. 50-1314. A copy of this petition is enclosed.

3. ☐ The information disclosure statement transmitted herewith is being filed *after* the period specified in §1.97(c), but before, or simultaneously with the payment of the issue fee. A statement specified in §1.97(e) and a fee set forth in §1.17(p) are included. 37 C.F.R. §1.97(d).

**§1.97(e) STATEMENT**

I, the person signing below, state:

- ☐ that each item of information contained in the information disclosure statement was first cited in the attached communication from a foreign patent office in a counterpart foreign application and that the communication is dated not more than three months prior to the filing of the statement. 37 C.F.R. §1.97(e)(1).

OR

- ☐ that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in §1.56(c) more than three months prior to the filing of the statement. 37 C.F.R. §1.97(e)(2).

**AND FEE**

- ☐ Attached is a fee set forth in 37 C.F.R. §1.17(p) for submission of an information disclosure statement under §1.97(d). (\$180.00).
4. ☒ If it should be determined that for any reason either an insufficient fee or an excessive has been paid, please charge any insufficiency or credit any overpayment necessary to ensure consideration of the information disclosure statement for the above-identified application to Deposit Account No. 50-1314. **A copy of this petition is enclosed.**
5. ☒ A list of 5 reference(s) is in the enclosed Form PTO-1449.

NON-ENGLISH LANGUAGE REFERENCES

- ☒ Also enclosed is a Corrected Form PTO-1449 submitted in order to correct typographical errors discovered on the form originally presented November 2, 2004.

In particular, in the third-listed reference (MENEZES), the pertinent pages are corrected to 1639-1646; in the eighth-listed reference (MATSUMOTO), the pertinent pages are corrected to 185-193; and in the seventeenth-listed reference (OHGISHI), the pertinent pages are corrected to 285-287 and the year of publication to 1999.

Since copies of each of these references were already submitted with the originally-submitted IDS, duplicate copies are not enclosed.

- ☐ The specification incorporates comments on the relevancy of Non-English language references.
- ☐ Set forth below are comments provided by the applicant's home country counsel on the relevancy of non-English language references:

Respectfully submitted,  
HOGAN & HARTSON L.L.P.

By: \_\_\_\_\_

Troy M. Schmelzer  
Registration No. 36,667  
Attorney for Applicant(s)

Date: February 8, 2006

Biltmore Tower  
500 South Grand Avenue, Suite 1900  
Los Angeles, CA 90071  
Telephone: (213) 337-6700  
Facsimile: (213) 337-6701

FORM PTO-1449

Docket Number (Optional)  
81942.0004Application Number  
09/708,263INFORMATION DISCLOSURE CITATION  
IN AN APPLICATION

Applicant

Kiyoshi Ogishi

Filing Date  
November 7, 2000Group Art Unit  
2134

(Use several sheets if necessary)

## U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

## FOREIGN PATENT DOCUMENTS

	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	Translation	
						YES	NO

## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	Ryuichi SAKAI, "Elliptic Curve Cryptosystems", (pp. 33-40), FAIT (Forum on Advanced Information Technology), Kyoto Institute of Technology, March 2000 and English language translation (pp. 1-24)
	Antonie JOUX, "A One Round Protocol for Tripartite Diffie-Hellman", W. Bosma (Ed.): ANTS-IV, LNCS 1838, pp. 385-393, July 2000
	R. BALASUBRAMANIAN, et al., "The Improbability That an Elliptic Curve Has Subexponential Discrete Log Problem under the Menezes-Okamoto-Vanstone Algorithm", J. CRYPTOLOGY (1998) 11: pp. 141-145
	Yasuyuki MURAKAMI, et al., "A New Probabilistic ID-Based Non-interactive Key Sharing Scheme", IEICE TRANS. FUNDAMENTALS, Vol. E83-A, No. 1, January 2000
	Ryuichi SAKAI, et al., "A New Class of Non-Interactive ID-Based Key Sharing Schemes and Its Performances", IEICE TRANS. FUNDAMENTALS, Vol. E78-A, No.1, January 1995

EXAMINER

DATE CONSIDERED

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP § 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.

<b>FORM PTO-1449 CORRECTED</b>  <b>INFORMATION DISCLOSURE CITATION IN AN APPLICATION</b>  <i>(Use several sheets if necessary)</i>	<b>Docket Number (Optional)</b> 81942.0004	<b>Application Number</b> 09/708,263
	<b>Applicant</b> OGISHI, et al.	
	<b>Filing Date</b> November 7, 2000	<b>Group Art Unit</b> 2134

**U.S. PATENT DOCUMENTS**

EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

**FOREIGN PATENT DOCUMENTS**

DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	Translation	
					YES	NO

**OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)**

	Joseph H. Silverman, "The Arithmetic of Elliptic Curves", Springer-Verlag, 1986, pp. 94-99
	OKAMOTO, et al., "Cipher/Zero Knowledge Proof/Number Theory", edited by Information Processing Society of Japan, Kyoritsu Suppan, 1995, pp. 185-197
	MENEZES, et al., "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field", IEEE Trans. Inf. Theory 39, pp. 1639-1646, 1993
	KANAYAMA, et al., "An Implementation of the MOV Reduction and the FR Reduction", SCIS '99, no.fl-1.4, Jan 1999, pp. 791-793
	BLAKE, et al., "Elliptic Curves in Cryptography", London Mathematical Society Lecture Note Series 265. Cambridge University Press, 1999, pp. 42-45, pp. 79-89
	HARAZAWA, et al., "Comparing the MOV and FR Reductions in Elliptic Curve Cryptography", vol.J82-A no.8, pp. 1278-1290
	M. KASAHARA, "Key Sharing System Based on the ID Information", vol. 47, no.2.pp. 141-145, Feb. 1993
	MATSUMOTO, et al., "On the Key Predistribution System: A Practical Solution to the Key Distribution Problem", Proceeding of Crypto'87, pp. 185-193, 1987
	H. TANAKA, "A Realization Scheme for the Identity-Based Cryptosystem", Proceeding of Crypto'87, pp. 340-349, 1987
	S. TSUJII, "An ID-Based Cryptosystem Based on the Discrete Logarithm Problem", IEEE Journal on Selected Areas in Communications, Vol.7, No. 4, 1989, pp. 467-473
	S. LANG, "Elliptic Curves Diophantine Analysis", Department of Mathematics, Yale University, Springer-Verlag. GTM112, 1978
	N. KOBLITZ, "Elliptic Curve Cryptosystems", Math. Comp. Vol.48. pp. 203-209. 1987
	V. MILLER, "Use of Elliptic Curves in Cryptography", Crypto85, pp.417-426. 1985
	J.A. SOLINAS, "An Improved Algorithm for Arithmetic on a Family of Elliptic Curves", Crypto97, pp. 357-371, 1997
	D. BAILEY, et al., "Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms", Crypto'98, pp. 472-485. 1998
	H. COHEN, et al., "Efficient Elliptic Curve Exponentiation Using Mixed Coordinates", AsiaCrypto'98, pp. 51-65, 1998

<b>EXAMINER</b>	<b>DATE CONSIDERED</b>
-----------------	------------------------

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP § 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.

FORM PTO-1449. CORRECTED

Docket Number (Optional)  
81942.0004Application Number  
09/708,263INFORMATION DISCLOSURE CITATION  
IN AN APPLICATION

(Use several sheets if necessary)

Applicant

OGISHI, et al.

Filing Date

November 7, 2000

Group Art Unit

2134

## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

OGISHI, et al., "Elliptic Curve Signature Scheme With No y Coordinate", SCIS'99, pp. 285-287, 1999

SATO, et al., "Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves", Comm. Math. Univ. Sancti Pauli, Vol. 47, pp. 81-92, 1998

N.P. SMART, "The Discrete Logarithm Problem on Elliptic Curves of Trace One", Journal of Cryptology, 1999, pp.193-196

I.A. SEMAEV, Evaluation of Discrete Logarithms In A Group of  $p$ -Torsion Points of An Elliptic Curve in Characteristic  $p$ , Math. Comp. Vol. 67, pp. 353-356, 1998FREY, et al., "A Remark Concerning  $m$ -Divisibility and The Discrete Logarithm in the Divisor Class Group of Curves", Math. Comp. Vol. 62, pp. 865-874, 1994R. SCHOOF, Elliptic Curves Over Finite Fields and the Computation of Square Roots Mod  $p$  Math. Comp. Vol. 44, pp. 482-494, 1985

F. MORAIN, "Building Cyclic Elliptic Curves Modulo Large Primes", EuroCrypt'91, pp. 328-336, 1991

EXAMINER

DATE CONSIDERED

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP § 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.